

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-146843

(43)Date of publication of application : 06.06.1997

(51)Int.Cl. G06F 12/14  
G06F 12/00

(21)Application number : 07-301029

(71)Applicant : FUJITSU LTD

(22)Date of filing : 20.11.1995

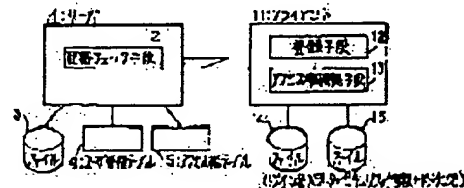
(72)Inventor : YAMAMOTO MASAHIKO

## (54) INFORMATION PROCESSOR

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To easily manage the security of a stored file by reading security information from the file for storing the security information for which access is requested at the time of access request, collating inputted information with read information and accessing the file when it is judged that an access right is present.

**SOLUTION:** A registration means 12 registers data, a domain name and the security information in the file and registers a prescribed domain name to a device, etc. An access right confirmation means 13 confirms the access right based on the domain name and the security information stored in the file. At the time of the access request, the access right confirmation means 13 reads the security information from the file for which the access is requested and collates the inputted information with the read security information, and when it is judged that the access right is present, the file is accessed.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

BEST AVAILABLE COPY

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office



(2)

特開平9-146843

## 【特許請求の範囲】

【請求項1】ファイルのセキュリティを行う情報処理装置において、

データを受信あるいはデータを作成したときに当該データを格納すると共に、セキュリティ情報を格納するファイルと、

アクセス要求時に、アクセス要求のあった上記ファイルからセキュリティ情報を読み出し、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときに当該ファイルのアクセスを行う手段を備えたことを特徴とする情報処理装置。

【請求項2】ファイルのセキュリティを行う情報処理装置において、

データを受信あるいはデータを作成したときに当該データを格納すると共に、ドメイン名を格納するファイルと、

アクセス要求時に、アクセス要求のあった上記ファイルからドメイン名を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致してアクセス権有と判明したときに当該ファイルのアクセスを行う手段を備えたことを特徴とする情報処理装置。

【請求項3】ファイルのセキュリティを行う情報処理装置において、

データを受信あるいはデータを作成したときに当該データを格納すると共に、ドメイン名およびセキュリティ情報を格納するファイルと、

アクセス要求時に、アクセス要求のあった上記ファイルからドメイン名およびセキュリティ情報を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致したときに、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときに当該ファイルのアクセスを行う手段を備えたことを特徴とする情報処理装置。

【請求項4】上記アクセス要求時に、アクセス要求のあった上記ファイルからセキュリティ情報を読み出し、入力されたユーザIDが読み出した所有者IDに一致したとき、入力されたグループ名が読み出したグループ名に一致しかつ読み出したグループに対するアクセス権が有のとき、あるいは入力されたグループ名が読み出したグループ名に一致しなかつ読み出したグループ以外に対するアクセス権が有のときに、当該ファイルのアクセスを行う手段とを備えたことを特徴とする請求項1あるいは請求項3記載の情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ファイルのセキュリティを行う情報処理装置に関するものである。

【0002】

【従来の技術】従来、セキュリティ機構を持たないクライアント（情報処理装置）では、ディスク装置に記憶さ

れたファイルや、FD（フロッピーディスク媒体）やMO（光磁気ディスク媒体）などに記憶されたファイル毎にパスワードを書き込み、ファイルのアクセス要求するときにパスワードを入力して一致したときのみアクセス許可してセキュリティを確保するようにしていた。

【0003】

【発明が解決しようとする課題】上述したセキュリティ機構を持たないクライアントでは、ファイル毎にパスワードを書き込んでおき、アクセス要求時に入力されたパスワードと一致したときにファイルアクセスを許可するようにしていたため、パスワードの設定、アクセス時のパスワード確認、パスワードの変更などに利用者にとって大きな負担となってしまう問題があった。また、ファイル毎にパスワードを書き込んでいたため、個人のファイルのセキュリティの管理に限られてしまい、会社組織の部署単位、課単位にアクセス権の有無などのセキュリティ管理を行い難いという問題があった。

【0004】本発明は、これら問題を解決するため、セキュリティ機構を持たない情報処理装置であってもファイル毎に所有者ID、グループ名、グループの権限の有無などのセキュリティ情報およびドメイン名を書き込んでおき、これらをもとにアクセス権の有無をチェックしてセキュリティを管理することを目的としている。

【0005】

【課題を解決するための手段】図1を参照して課題を解決するための手段を説明する。図1において、登録手段12は、データ、ドメイン名、およびセキュリティ情報をファイルに登録したり、所定のドメイン名を装置に登録したりなどするものである。

【0006】アクセス権確認手段13は、ファイルに格納されているドメイン名およびセキュリティ情報をもとにアクセス権を確認するものである。次に、動作を説明する。

【0007】アクセス要求時に、アクセス権確認手段13がアクセス要求のあったファイルからセキュリティ情報を読み出し、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときにファイルのアクセスを行うようにしている。

【0008】また、アクセス要求時に、アクセス権確認手段13がアクセス要求のあったファイルからドメイン名を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致してアクセス権有と判明したときにファイルのアクセスを行うようにしている。

【0009】また、アクセス要求時に、アクセス権確認手段13がアクセス要求のあったファイルからドメイン名およびセキュリティ情報を読み出し、装置自体に登録されているドメイン名と読み出したドメイン名とが一致したときに、入力された情報と読み出したセキュリティ情報とを照合してアクセス権有と判明したときにファイルのアクセスを行うようにしている。

【0010】また、アクセス要求時に、アクセス権確認手段13がアクセス要求のあったファイルからセキュリティ情報を読み出し、入力されたユーザIDが読み出した所有者IDに一致したとき、入力されたグループ名が読み出したグループ名に一致しかつ読み出したグループに対するアクセス権が有るとき、あるいは入力されたグループ名が読み出したグループ名に一致しなかつ読み出したグループ以外に対するアクセス権が有るときに、ファイルのアクセスを行うようにしている。

【0011】従って、セキュリティ機構を持たない情報処理装置であっても、ファイル毎に所有者ID、グループ名、グループの権限の有無などのセキュリティ情報およびドメイン名を書き込んでおき、アクセス権確認手段13がこれらをもとにアクセス権の有無をチェックしてセキュリティを管理することが可能となる。

【0012】

【発明の実施の形態】次に、図1から図8を用いて本発明の実施の形態および動作を順次詳細に説明する。

【0013】図1は、本発明のシステムブロック図を示す。図1において、サーバ1は、回線を介して1つあるいは複数のクライアント11と接続しファイルの一括管理するものであって、ここでは、資格チェック手段2などから構成されるものである。

【0014】資格チェック手段2は、クライアント11から回線を介して接続されたときに、ユーザの資格をチェックするものであって、例えばユーザID、パスワードなどでその資格をチェックするものである。

【0015】ファイル3は、管理するデータを格納するものである。ユーザ管理テーブル4は、ユーザを管理するものであって、例えばユーザIDに対応づけてパスワードおよび属するグループ名（例えば総務課）などを予め登録するものである（図2参照）。

【0016】アクセス権テーブル5は、ユーザのアクセス権を管理するものであって、例えばディレクトリあるいはそのファイル毎に所有者、グループ、その他などの情報を登録するものである（図3参照）。

【0017】クライアント11は、サーバ1に回線を介して接続して各種業務処理を行うものであって、ここでは、登録手段12、およびアクセス権確認手段13などから構成されるものである。

【0018】登録手段12は、データ、ドメイン名、およびセキュリティ情報をファイルに登録したり、ドメイン名を空欄に登録したりなどするものである（図4ないし図7を用いて後述する）。

【0019】アクセス権確認手段13は、ファイルに格納されているドメイン名およびセキュリティ情報をもとにアクセス権を確認するものである（図6ないし図8を用いて後述する）。

【0020】ファイル14は、クライアント11という装置に対応づけてドメイン名を登録するものである。フ

ァイル15は、データにセキュリティ情報（所有者ID、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）およびドメイン名などを登録するものである。

【0021】図2は、本発明のユーザ管理テーブル例を示す。このユーザ管理テーブル4は、図示のように、ユーザIDに対応づけて下記の項目を予め登録したものである。

【0022】

- ・ユーザID: U01
- ・パスワード: 011
- ・グループ名: X
- ・その他

ここで、ユーザIDは、クライアント11あるいはその利用者に対して一意に割り当てられたIDである。グループ名は、利用者の属するグループ名である。

【0023】以上のように、ユーザIDに対応づけてパスワードおよびグループ名などを予めユーザ管理テーブル4に登録しておくことにより、クライアント11から回線を介してサーバ1に接続し、サーバ1のファイル3からデータをダウンロードしようとするときに、資格チェック手段2が資格をチェックしてOKのときにファイルおよびセキュリティ情報（所有者ID、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）をダウンロードすることが可能となる。

【0024】図3は、本発明のアクセス権テーブル例を示す。このアクセス権テーブル5は、サーバ1がセキュリティ管理するファイル3について、ディレクトリ毎にセキュリティ情報（所有者ID、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）および各ファイル毎のセキュリティ情報（所有者ID、グループ名、グループに対するアクセス権の有無、その他に対するアクセス権の有無など）を予め登録したものである。このセキュリティ情報は、サーバ1の管理者が適宜登録する。

【0025】以上のように、サーバ1が管理するファイルについて、ディレクトリ毎にセキュリティ情報、およびファイル毎にセキュリティ情報を付加してセキュリティを管理し、クライアント11にダウンロードするときにファイルのデータにこのセキュリティ情報を付加して送信する。受信したクライアントではこのセキュリティ情報をファイル内のデータに付加しておく。

【0026】次に、図4のフローチャートに示す順序に従い、図1ないし図3の構成のもとで、サーバ1からファイルをクライアント11にダウンロードしてセキュリティ情報を当該ファイル書き込むときの手順を詳細に説明する。

【0027】図4は、本発明のダウンロードフローチャート（セキュリティ情報の書き込み）を示す。図4にお

いて、S1は、サーバに接続し、ユーザ認証する。これは、クライアント11が回線を介してサーバ1に接続し、ユーザID、パスワードを入力して送信し、サーバ1の資格チェック手段2がユーザ管理テーブル4を参照してユーザIDに対応づけてパスワードが登録され、資格があるか否かをチェックする。OKのときにS2に進む。

【0028】S2は、ファイル受信する。これは、S1で資格チェックしてOKとなったので、サーバ1がファイル3をダウンロードし、クライアント11がファイルを受信する。

【0029】S3は、セキュリティ情報を受信する。これは、S2でファイルをサーバ1がダウンロードしてクライアント11が受信したことに続き、サーバ1がダウンロードしたファイルのアクセス権テーブル5を参照してセキュリティ情報として、

- ・所有者ID:A
- ・グループ名:X
- ・グループに対するアクセス権:有/無
- ・その他に対するアクセス権:有/無
- ・その他

をダウンロードし、クライアント11が受信する。ここで、セキュリティ情報は、図3のアクセス権テーブル5を参照し、ダウンロードしたファイルのディレクトリおよび当該ファイルのセキュリティ情報の両者を読み出し、より厳しい値（AND条件の値）を生成しセキュリティ情報としてクライアント11にダウンロードし、セキュリティ管理の完備したサーバ1からセキュリティ管理の無いクライアント11にこのセキュリティ情報を渡したことになる。

【0030】S4は、ファイル内にセキュリティ情報を書き込む。これは、クライアント11がS2で受信したファイルに、S3で受信したセキュリティ情報を当該ファイルに書き込む。

【0031】以上によって、セキュリティ管理の完備したサーバにおけるファイルのセキュリティ情報を、ダウンロードを受けたクライアント11でファイル自身に当該セキュリティ情報を書き込み、セキュリティ管理する準備が完了したこととなる。

【0032】図5は、本発明のダウンロードフローチャート（ドメイン名の書き込み）を示す。ここで事前にドメイン名を登録しておく。例えばクライアント11を起動した管理者が画面上からドメイン名を入力して当該クライアント11のファイル14にドメイン名、例えば“営業部”を登録する。これにより、以降は利用者は、同一のドメイン名のファイルしかアクセスできないようにロックされることとなる。

【0033】図5において、S11は、サーバに接続する。そして、既述した図4のS1と同様に資格チェックを受け、OKのときにS12に進む。S12は、ファイ

ル受信する。これは、クライアント11がサーバ1からファイルを受信する。

【0034】S13は、クライアントがファイルを作成する。S14は、ファイル内にドメイン名を書き込む。これは、S12でサーバ1からダウンロードされて受信したファイル、あるいはS13でクライアント内で作成したファイルについて、ドメイン名を書き込む。ドメイン名は、例えば後述する図9に示すように、このファイルのアクセスを許可するドメイン名、例えば“営業部”、“総務部”、“経理部”などをファイルに書き込み、当該ドメイン名が書き込まれたファイルについて、同一のドメイン名が予め登録されたクライアント（端末）11しか当該ファイルをアクセスできないようにクライアント11のアクセス権確認手段13が制御する。

【0035】以上によって、ダウンロードを受けたファイルあるいは作成したファイルに対してドメイン名を書き込み、当該ドメイン名の登録されたクライアント（端末）11しか当該ファイルをアクセスできないようにアクセス権確認手段13が制御を行うことが可能となる。

【0036】図6は、本発明のダウンロードしたファイルに対するアクセスフローチャートを示す。図6において、S22は、サーバに接続する。そして、ユーザ認証する。これは、クライアント11が回線を介してサーバ1に接続し、ユーザID、パスワードを入力して送信し、サーバ1の資格チェック手段2がユーザ管理テーブル4を参照してユーザIDに対応づけてパスワードが登録され、資格があるか否かをチェックする。OKのときにS23に進む。

【0037】S23はユーザIDが所属しているグループ名を受信する。これは、既述した図2のユーザ管理テーブル4を参照し、ユーザIDが所属しているグループ名を取り出して受信する。

【0038】S24は、サーバとの接続を切断する。以上のS21からS24によって、クライアント（端末）11に、サーバから当該ユーザIDのグループ名を受信する。

【0039】S25は、ファイルをアクセスする。これは、あるユーザIDの利用者がクライアント11の保持するあるファイル15をアクセスしようとする。S26は、ドメイン名が一致か判別する。これは、S25でアクセスしようとしたファイル15に書き込まれているドメイン名と、当該クライアント（端末）11に管理者が事前に登録したドメイン名とが一致するか判別する。YESの場合には、S27に進む。一方、NOの場合には、ドメイン名が一致しなく当該ファイルへのアクセスが許可できないので、S33でアクセス不可とし、S34エラー処理を行い、終了する。

【0040】S27は、ユーザIDとファイル内の所有者が一致か判別する。これは、S25でアクセスしようとした利用者のユーザIDと、アクセスしようとしたフ

ファイル内に書き込まれている所有者IDとが一致し、アクセス権がありか判別する。YESの場合には、アクセス権有と判明したので、S31でアクセス可と判定し、S32でアクセスを行う。一方、S27のNOの場合には、所有者でないと判明したので、S28に進む。

【0041】S28は、グループ名とファイル内のグループ名が一致か判別する。これは、S23で受信したユーザIDが所属するグループ名と、S25でアクセスしようとしたファイル内に書き込まれているグループ名と一致か判別する。YESの場合には、更に、S29でファイル内に書き込まれているグループに対するアクセス権の有無を読み出し、有のときにS31でアクセス可と判定しS32でアクセスし、無のときにS33でアクセス不可と判定しS34でエラー処理し終了する。一方、S28のNOの場合には、更にS30でファイル内に書き込まれているその他に対するアクセス権の有無を読み出し、有のときにS31でアクセス可と判定しS32でアクセスし、無のときにS33でアクセス不可と判定しS34でエラー処理し終了する。

【0042】以上によって、ファイル内に書き込まれているドメイン名、所有者名、グループ名、グループに対するアクセス権の有無、およびその他に対するアクセス権の有無に従い、アクセス権有りと判明したとき(S27のYES、S28のYESかつS29の有、S28のNOかつS30の有のいずれかのとき)に、ファイルのアクセスを許可し、セキュリティ機能のないクライアント(端末)11であっても、本発明によってサーバ1が持つセキュリティ情報に従ったセキュリティ管理を行うことが可能となる。

【0043】図7は、本発明のドメイン名登録フローチャートを示す。これは、既述した図5の事前ドメイン名登録の詳細手順である。図7において、S41は、管理システムのインストールする。これは、図1のクライアント11で管理システム(登録手段12、アクセス権確認手段13などの管理システム)をインストールする際に、ドメイン名およびアクセス権のセキュリティの有無について、いずれか一方、あるいは両者をチェックするかの区別を登録する。これにより、ドメイン名のみによるアクセス権のチェック、セキュリティ情報のみによるアクセス権のチェック、あるいは両者によるアクセス権のチェックのいずれかがインストール時などに設定されることとなる。

【0044】S42は、ドメイン名を入力する。S43は、ドメイン名を登録する(図1のファイル14を作成する)。これらS42およびS43は、管理者がクライアント(端末)11に管理システムをインストールする際に、アクセス権のチェックする仕方(ドメイン名のみ、セキュリティ情報のみ、あるいは両者)を設定する。

【0045】以上によって、クライアント(端末)11

のインストール時などに管理者がドメイン名、セキュリティ情報、あるいは両者によるアクセス権のチェックを行うかを任意に設定することが可能となる。

【0046】図8は、本発明のファイルアクセスフローチャートを示す。これは、ドメイン名によってアクセス権をチェックするときの手順である。図8において、S51は、ファイルのアクセスをしようとする。

【0047】S52は、ドメイン名とファイル内のドメイン名とが一致か判別する。これは、利用者が操作したクライアント11に登録されているドメイン名と、S51でアクセスしようとしたファイルに書き込まれているドメイン名とが一致か判別する。YESの場合には、一致してアクセス権有と判明したので、S53でアクセス可と判定し、S54でアクセスを行う。一方、NOの場合には、一致しなくアクセス権無と判明したので、S55でアクセス不可と判定し、S56でエラー処理を行い、終了する。

【0048】図9は、本発明のドメインの説明図を示す。ここで、ドメインは特定の部署が使用するクライアント(端末)11に登録して当該ドメイン名が書き込まれたファイルのアクセスのみを可能し、クライアント11とファイルとをドメイン名でロックするようにしたものである。ここでは、図示のように

・ドメイン1として、営業部のクライアント(端末)11を3台割り当て、既述した図7のフローチャートに従い、同一のドメイン名“ドメイン1”を当該クライアント11に登録する。

【0049】・ドメイン2として、総務部のクライアント(端末)11を3台割り当て、既述した図7のフローチャートに従い、同一のドメイン名“ドメイン2”を当該クライアント11に登録する。

【0050】・ドメイン3として、経理部のクライアント(端末)11を3台割り当て、既述した図7のフローチャートに従い、同一のドメイン名“ドメイン3”を当該クライアント11に登録する。

【0051】以上のように、ドメイン名“ドメイン1”、“ドメイン2”、“ドメイン3”をそれぞれ営業部、総務部、経理部が利用するクライアント(端末)11に図7のフローチャートに従い登録することにより、これら各クライアント(端末)11は、媒体中のファイルのうち、各自のドメイン名が一致するファイルのみをアクセスすることが可能となり、他のクライアント11はアクセスできず、セキュリティを確保することが可能となる。

【0052】

【発明の効果】以上説明したように、本発明によれば、セキュリティ機構を持たない情報処理装置であっても、ファイル毎に所有者ID、グループ名、グループの権限の有無などのセキュリティ情報およびドメイン名を書き込んでおき、アクセス権確認手段13がこれらをもとに

(6)

特開平9-146843

アクセス権の有無をチェックする構成を採用しているため、ファイル毎にセキュリティを管理することができ、これらにより、セキュリティ機構を持たないクライアント（端末）であっても、ファイルにセキュリティ情報およびドメイン名を書き込んでおき、媒体などに格納されたファイルのセキュリティを簡易に管理することが可能となる。

【図面の簡単な説明】

【図1】本発明のシステムブロック図である。

【図2】本発明のユーザ管理テーブル例である。

【図3】本発明のアクセス権テーブル例である。

【図4】本発明のダウンロードフローチャート（セキュリティ情報の書き込み）である。

【図5】本発明のダウンロードフローチャート（ドメイン名の書き込み）である。

【図6】本発明のダウンロードしたファイルに対するアクセスフローチャートである。

【図7】本発明のドメイン名登録フローチャートである。

【図8】本発明のファイルアクセスフローチャートである。

【図9】本発明のドメインの説明図である。

【符号の説明】

1：サーバ

2：資格チェック手段

3：ファイル

4：ユーザ管理テーブル

5：アクセス権テーブル

11：クライアント（端末）

12：登録手段

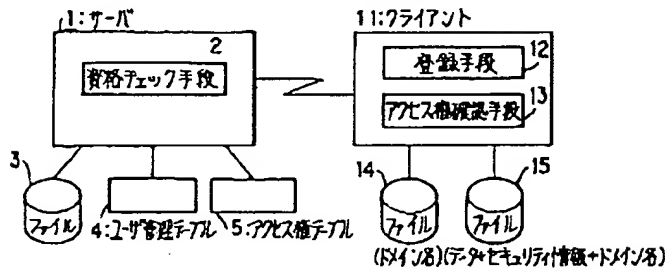
13：アクセス権確認手段

14：ファイル（ドメイン名）

15：ファイル（データ+セキュリティ情報+ドメイン名）

【図1】

本発明のシステムブロック図



【図2】

本発明のユーザ管理テーブル例

4		
ユーザID	パスワード	グループ
U01	011	X
⋮	⋮	⋮

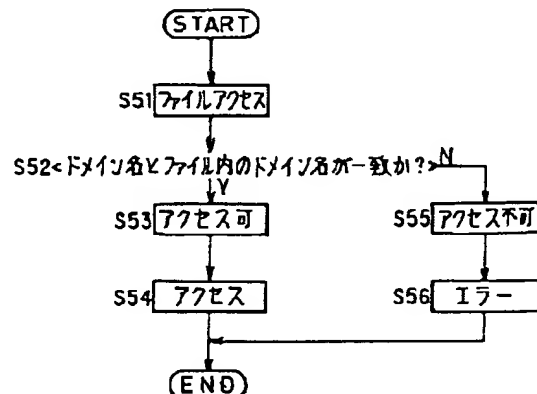
【図3】

本発明のアクセス権テーブル例

5		
ディレクトリXX	ファイルXXX	所有者
・所有者		・グループ：有/無
・グループ：有/無		・その他：有/無
・その他：有/無		
		⋮
		⋮

【図8】

本発明のファイルアクセスフローチャート



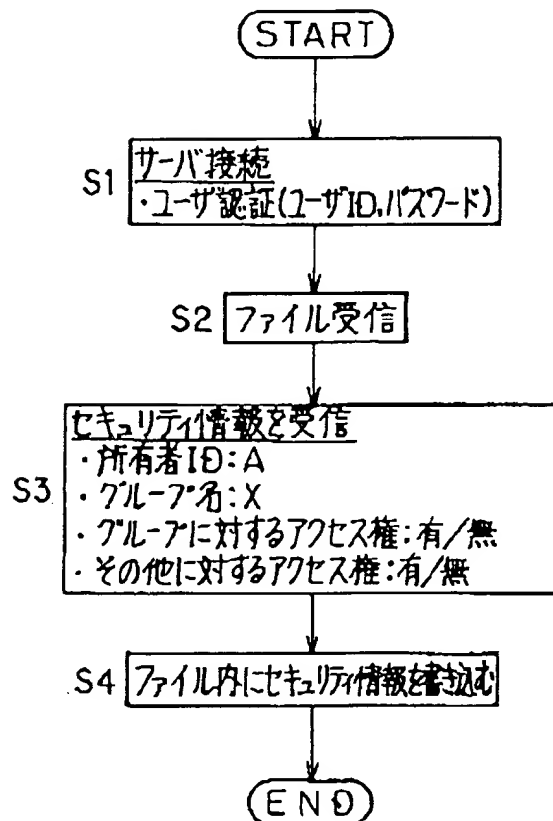


(7)

特開平9-146843

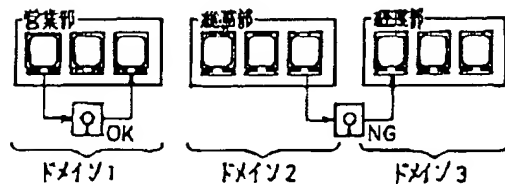
【図4】

本発明のダウンロードフローチャート(セキュリティ情報の書き込み)



【図9】

本発明のドメインの説明図

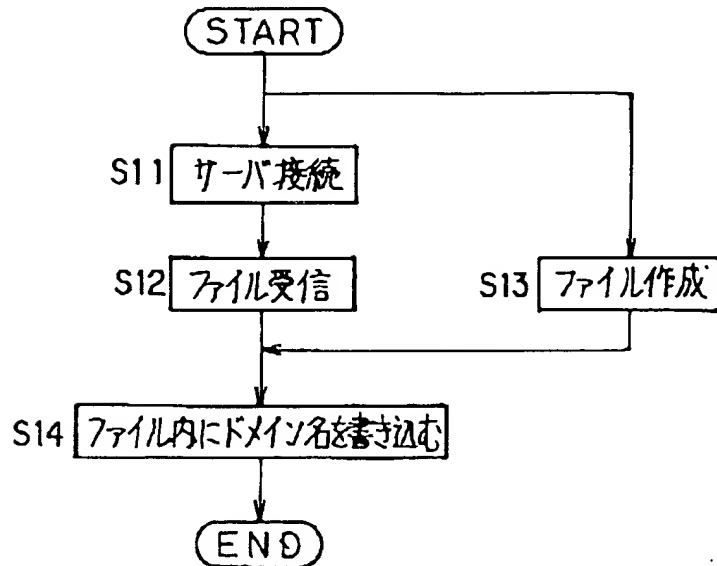


(8)

特開平9-146843

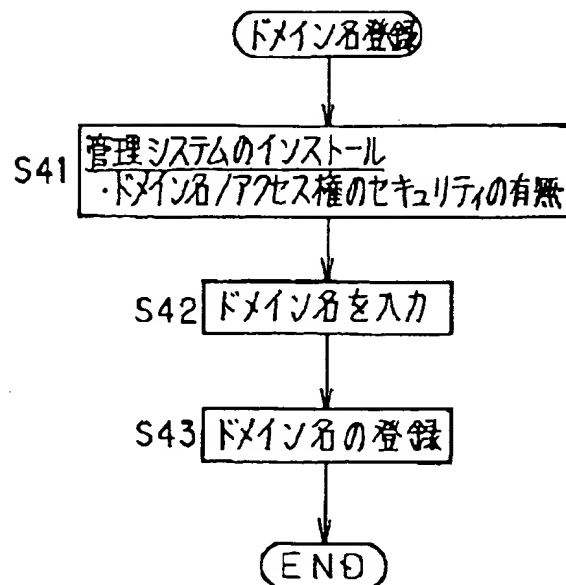
【図5】

本発明のダウンロードフローチャート(ドメイン名の書き込み)



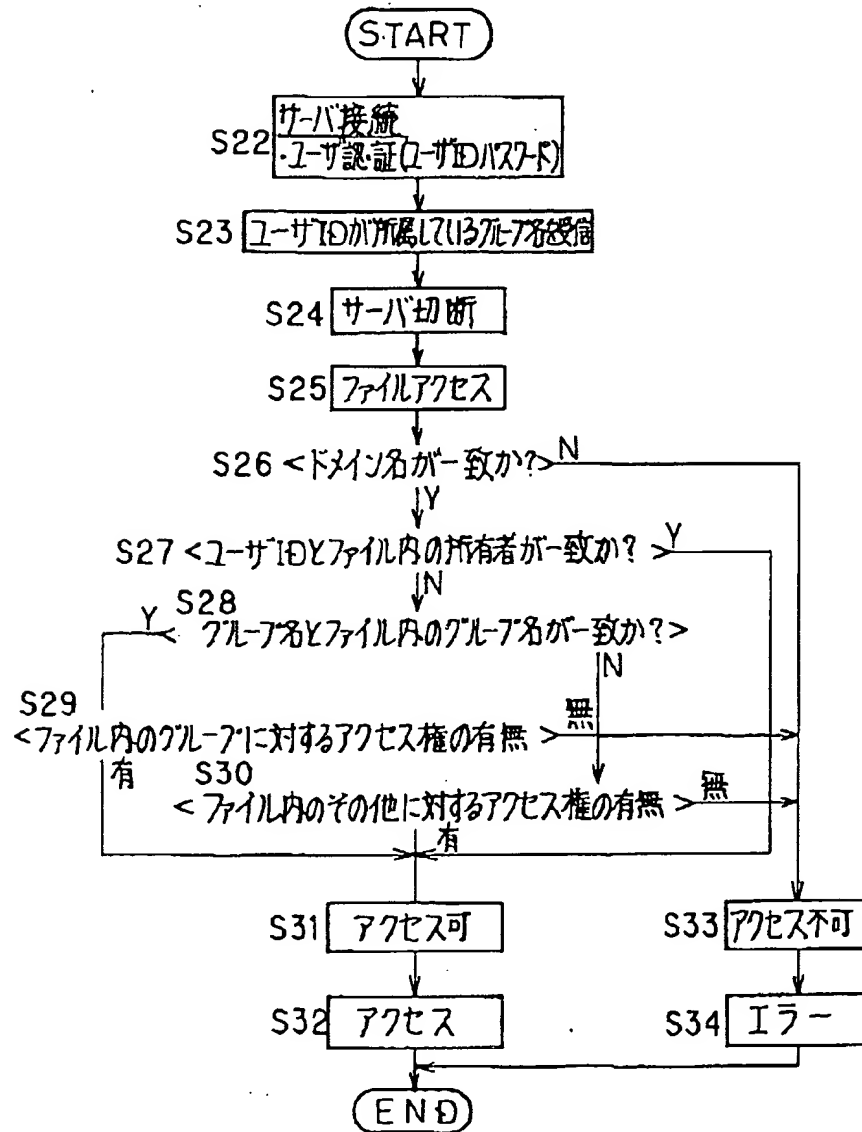
【図7】

本発明のドメイン名登録フローチャート



【図6】

本発明のダウンロードしたファイルに対するアクセスフローチャート



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**